

A geometric protocol for cryptography with cards

Andrés Cordón–Franco, Hans van Ditmarsch,
David Fernández–Duque, and Fernando Soler–Toscano*

July 25, 2012

Abstract

In the Russian cards problem, Alice, Bob and Cath draw three, three and one cards, respectively, from a deck of seven. Alice and Bob must then communicate their entire hand to each other, without Cath learning the owner of a single card. Unlike many traditional problems in cryptography, however, they are not allowed to hide or codify the messages they exchange from Cath. The problem is then to find methods through which they can achieve this. One elegant solution, due to Atkinson, considers the cards as points in a finite projective plane.

In this paper we consider the *generalized* Russian cards problem, where the number of cards that each player draws is a, b and c , respectively, from a deck of $a + b + c$ cards. We propose a general solution in the spirit of Atkinson’s, although based on finite vector spaces, and call it the “colouring protocol”, as it involves colourings of affine subsets.

Our main results show that the colouring protocol provides a solution to the generalized Russian cards problem in cases where a is a power of a prime and either

1. $c < a$ and $b = O(ac)$ or

*Emails and affiliations: {acordon,hvd,dfduque,fsoler}@us.es, University of Sevilla, Spain. Hans van Ditmarsch is also affiliated to IMSc, Chennai, India, as a research associate.

2. $c = O(a^2)$ and $b = O(c^2)$.

This improves substantially on the collection of parameters for which solutions are known. In particular, it is the first solution which allows the eavesdropper to have more cards than one of the players.

1 Introduction

In this article we present protocols based on finite vector spaces for three card players exchanging secrets. The general idea is that two of the three agents wish to share confidential information and actively cooperate in doing so, whereas the third agent plays the role of an eavesdropper. As is common practice in the cryptography literature, we will henceforth call the agents exchanging secrets Alice and Bob. The eavesdropper (usually called Eve) is able to hear all communications, and Alice and Bob are aware of that. We call her Cath. As a consequence, in such information-exchanging protocols between Alice and Bob, Cath typically acquires quite a bit of data, but not enough to be able to deduce any secrets; the latter a requirement for a protocol to be successful.

Let us describe the problem we are concerned with:

The generalized Russian cards problem

Alice, Bob and Cath each draw a, b and c cards, respectively, from a deck of size $a + b + c$. All players know which cards were in the deck and how many of them the other players drew, but each player may only see the cards in their own hand.

Alice and Bob, however, want to know exactly which cards the other holds. Moreover, they do not want for Cath to learn who holds *any* card whatsoever, aside of course from her own cards.

However, they may only do so by making true, clear, public announcements, so that Cath can learn all the information that they exchange.

Can Alice and Bob achieve this?

The generalized Russian cards problem is parametrized by the triple (a, b, c) , which we will often call the *size* of the deal. A (possible) solution to

the generalized Russian cards problem is a *protocol*; that is, a series of steps that Alice and Bob must follow in order to achieve their goal. Later we shall give some constraints on what constitutes a valid or successful protocol.

Solutions to the generalized Russian cards problem can often be formulated in purely combinatorial or even geometric terms. One protocol that is known, and we shall discuss below, views cards as points in finite projective planes. This has inspired the present work, whose aim was to find a variant or generalization which solved more instances of the problem. The protocol we propose is, to the best of our knowledge, the first solution to the generalized Russian cards problem which works in cases where Cath holds more cards than Alice.

Let us first present the projective geometry protocol, suggested by Mike Atkinson in 2001. Consider players Alice and Bob each drawing three cards from a deck of seven cards, while Cath gets the remaining card. One way for Alice and Bob to communicate their cards to each other by way of public announcements, without informing Cath of any of their cards, is when Alice announces that her hand of cards is a line in a projective plane consisting of seven points (cards). Or, to be precise, Alice assigns a point in the projective plane to each card in such a way that her own hand forms a line, and announces

If all the cards in the deck are arranged in the projective plane in the way I am telling you, then my hand forms a line.

After this, it suffices for Bob to announce Cath's card. Why does this work?

Suppose that the cards are numbered $0, 1, \dots, 6$, that Alice holds the cards $0, 1$ and 2 , Bob holds $3, 4$, and 5 , and therefore Cath holds 6 . Alice announces: "My hand of cards corresponds to one of the lines in the projective plane whose lines are $012, 034, 056, 135, 146, 236$, and 245 ." (See Figure 1.) Bob then announces: "Cath holds 6 ." After Alice's announcement, Cath, who holds card 6 , can eliminate from the seven triples the ones containing 6 : $056, 146$, and 236 . The remaining hands are: $012, 034, 135$ and 245 . Cath therefore cannot deduce that Alice has 0 , because 135 is a possible hand of Alice. She also cannot deduce that Alice does not have 0 , because Alice's actual hand 012 is also a possible hand. And so on, for all possible cards of Alice. Because Alice does not know which card Cath actually holds, we have to make sure that the protocol would work even if Cath held a different one;

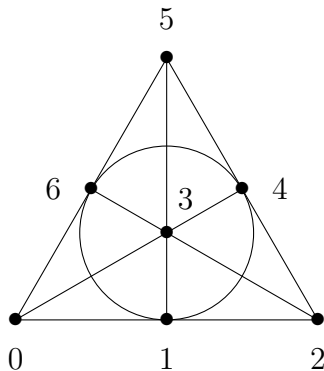


Figure 1: Alice holds a line in the 7-point projective plane

otherwise, Alice would risk giving a secret away to Cath, yet we are only interested in protocols that work unconditionally.

Meanwhile, Bob learns Alice's cards from her announcement, because all but 012 contain either a 3, a 4, or a 5. Again, we have to do this for all card triples xyz , not just for Bob's actual hand 345. In the end, he knows Cath's card and can announce it, from which Alice also learns the entire deal of cards.

There are other protocols for this setting of card dealing players; see e.g. [1, 3, 9]. A possibly better-known solution to the riddle make Alice and Bob both announce the sum of their cards modulo 7 (i.e., modulo the number of cards in the pack); this was the proposed solution when the problem appeared in the Moscow Mathematics Olympiad in 2000 [5]. This protocol works in many more cases, provided that Cath holds only one card [2].

The Russian cards problem itself is much older and originates with Kirkman [4]. There, the solution takes the form of a *design*, a collection of subsets of a given set that satisfies certain regulaties [8]. The design consists of seven triples — and accidentally these are the lines that form the projective geometric plane. Cryptography based on card deals is also investigated in various other, not necessarily related publications, such as [6, 7].

The instances for which the generalized Russian cards problem has known solutions are the following:

1. The case $(3, 3, 1)$ has been extensively studied and has many solutions [4, 5].

2. The case $(4, 4, 2)$ has an unusual solution given in [10].
3. All cases $(a, 2, 1)$ provided $a \equiv 0, 4 \pmod{6}$ have been solved in [1].
4. All cases¹ $(a, b, 1)$ with both $a, b > 2$ have been solved in [2].
5. If $c + 1 < a$ then there is a solution for $b = O(a^2)$, somewhat in the spirit of Atkinson's [1].

In this paper, we provide solutions for the cases where a is a power of a prime and either

6. $c + 1 < a$ and $b = O(ac)$, thus improving on 5 when $c \ll a$ or
7. $b = O(c^2)$ and either $c = O(a^{3/2})$ or $c = O(a^2)$, the first known solutions for $c > a$.

Let us now consider a simple example of the protocol we will present. Suppose there are 25 cards, of which Alice holds 5, Bob 17 and Cath 3. A suitable protocol for Alice and Bob to inform each other of their cards is, similar to the above, that Alice first announces that her cards are a line in a two-dimensional vector space with characteristic five, i.e., \mathbb{F}_5^2 . After this, Bob announces Cath's cards.

The 25 cards in the deck D could be named $0, 1, \dots, 24$, or they could be all clubs and all hearts except for the ace of hearts, or they could be dominoes instead of cards. The only thing that matters is that the number of cards is the same as the number of points in \mathbb{F}_5^2 . Alice's announcement can then be represented as a bijection $f : D \rightarrow \mathbb{F}_5^2$, where \mathbb{F}_5^2 may be represented as $\{ij \mid 0 \leq i, j \leq 4\}$.

Why does this inform Bob of Alice's cards? Consider the typical configuration in Figure 2, left-hand side, where Alice's cards are represented as \blacksquare , Bob's as \circ and Cath's as \blacktriangle . As before, Alice's announcement rules out some possibilities for her hand. She cannot have, for example, $\{00, 11, 22, 23, 24\}$.

From Bob's perspective, Alice's announcement is sufficient for him to determine her hand. Suppose that A, C are the sets of cards that Alice and Cath hold, respectively. Then, $A \cup C$ contains eight points, and thus cannot contain two different lines; as two lines intersect in at most one point, any set in \mathbb{F}_5^2 containing two lines must have at least nine elements.

¹This subsumes the case $(3, b, 1)$ for $b \geq 3$, also covered previously in [1].

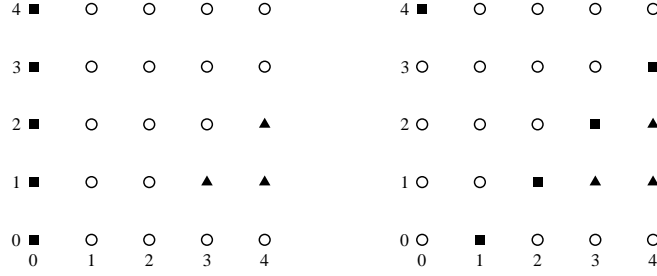


Figure 2: Card deals in \mathbb{F}_5^2

On the other hand, for Cath, this information is insufficient to determine the ownership of a single card not in her possession. As an example, let us take card 00 of Alice's. Observe that there is a line in \mathbb{F}_5^2 not containing 00 but still avoiding Cath's cards 31, 41, and 42, for example as in the right-hand side of Figure 2. More generally, for any subset of three points in \mathbb{F}_5^2 and any other point x , we can find a line avoiding these three points and containing x and another such line not containing x .

The same trick works if Cath has fewer than three cards, but if she has four cards we cannot rule out that a nine-point set contain two lines. And if she has even more than four (and maybe even more cards than Alice) this only gets worse. We then need another trick, adding more steps to the protocol.

Suppose that Cath has as many cards as Alice or perhaps even more. Then, after Alice maps the deck into a finite vector space \mathcal{V} (which in this case will usually be quite a bit larger than \mathbb{F}_3^2), Bob may not be able to immediately distinguish which of the lines contained in $A \cup C$ is Alice's. What Bob will do is to colour the lines of \mathcal{V} , so that each line that Alice might have has is assigned a different colour, and ask, *Alice, what colour is your hand?*

Of course, Bob must be careful in how he colours the lines! If he uses too many colours, for example a distinct colour for each line in \mathcal{V} , Cath may learn exactly which line Alice holds. And, if he does not use enough colours, he may still not know which cards belong to whom, as maybe Cath also holds a line of the same colour. But it is possible to give conditions under which a colouring is *suitable* for the protocol to be successful.

This is the basic idea of the *colouring protocol*, which we shall describe formally in Section 3, after introducing some preliminary notions about pro-

protocols in Section 2. The protocol we shall present does not assume that Alice holds a line, but rather a linear subset of \mathcal{V} of any dimension. Although our protocol is based on finite vector spaces, it is essentially a generalization of Atkinson's, with our example based on \mathbb{F}_5^2 being a special case. In Section 3 we will also prove that the protocol provides a solution to the generalized Russian cards problem.

However, this result will be based on the assumption that the protocol is executable, which is not the case for deals of arbitrary size (a, b, c) . The following sections will study special cases in which the protocol may be applied; in Section 4 we study the case when Alice's hand forms a hyperplane in \mathcal{V} , while Section 5 studies the case when Alice's cards form a line. In both cases, we give explicit bounds on the parameters which ensure that the colouring protocol is executable.

2 Card protocols

Throughout this paper, we shall assume that D is a fixed, finite set of d "cards". A *card deal* is a partition (A, B, C) of D ; the deal has *size* (a, b, c) if A is an a -set, B a b -set and C a c -set, where by " x -set" we mean a set of cardinality x . We think of A as the *hand* of Alice, or that Alice *holds* A ; similarly, B and C are the hands of Bob and Cath, respectively. In general we may simply assume that $D = \{1, \dots, a + b + c\}$, and define $\text{Deal}(a, b, c)$ to be the set of partitions of D of size (a, b, c) .

Central to this text is the notion of *protocol*. Roughly, a protocol is a family of rules or instructions that Alice and Bob must follow in order to send out a sequence of public announcements. It suffices to think of an announcement as a pair $\alpha = (i, \phi)$, where i is either Alice or Bob and ϕ is a 'token'. Usually ϕ is taken to be a statement about the game but it could also be another speech act such as asking a question or saying "Pass".

A sequence

$$\vec{\alpha} = (i_0, \phi_0), (i_1, \phi_1), \dots, (i_n, \phi_n)$$

is a *run*. We shall write $\text{Ann}(a, b, c)$ for the set of announcements and $\text{Run}(a, b, c)$ for the set of runs, including the empty sequence.

Players only have direct knowledge of their own cards, and thus at the beginning of the game should not be able to distinguish between different deals where they hold the same hand; thus, from Alice's perspective, (A, B, C) is

indistinguishable from (A', B', C') if $A = A'$, and we write

$$(A, B, C) \stackrel{Alice}{\sim} (A', B', C').$$

We may define analogous equivalence relations for Bob and Cath. After other agents have made announcements, each agent may incorporate them into their knowledge, including ‘higher-order’ reasoning about others’ intentions and knowledge.

Formally, we may define a protocol as follows:

Definition 2.1 (Protocol). *Let $\text{Deal} = \text{Deal}(a, b, c)$, $\text{Ann} = \text{Ann}(a, b, c)$ and $\text{Run} = \text{Run}(a, b, c)$.*

A protocol (with (a, b, c) as parameters) is a function

$$\pi : \text{Deal} \times \text{Run} \rightarrow \mathcal{P}(\text{Ann})$$

such that, for every deal δ and run $\vec{\alpha}$,

- 1. if $(i, \phi), (i', \phi') \in \pi(\delta, \vec{\alpha})$, then $i = i'$*
- 2. if $(i, \phi) \in \pi(\delta, \vec{\alpha})$ and $\delta' \stackrel{i}{\sim} \delta$, then $\pi(\delta', \vec{\alpha}) = \pi(\delta, \vec{\alpha})$.*

Thus once a deal has been given, a protocol assigns to each run a player who is to make the next announcement, and a set of “allowed announcements” for the player to make. Intuitively, the first property says that the next player to make a move is always determined (although the content of the announcement may vary); the second, that players may only choose their announcements based on the data they have access to.

Protocols are non-deterministic in principle and hence may be executed in many ways; an *execution of a protocol* is a pair $(\delta, \vec{\alpha})$, where δ is a deal, $\vec{\alpha} = (i_0, \phi_0), \dots, (i_n, \phi_n)$ a run and, for all $k < n$,

$$(i_{k+1}, \phi_{k+1}) \in \pi(\delta, (i_0, \phi_0), \dots, (i_k, \phi_k)).$$

So far, we have described protocols in general but have said little about their *objectives*. Indeed, a protocol as described above may very well give little useful information to Alice or Bob, or perhaps give too much information to Cath. Let us now describe what it means for a protocol to be successful in our setting.

The first objective we have is for Alice and Bob to know each other’s cards (and hence the entire deal) after its execution:

Definition 2.2 (informativity). *A run $((A, B, C), \vec{\alpha})$ is informative for Alice if there is no other run $((A, B', C'), \vec{\alpha})$ with $C' \neq C$.*

Similarly, a run $((A, B, C), \vec{\alpha})$ is informative for Bob if there is no other run $((A', B, C'), \vec{\alpha})$ with $C' \neq C$.

A protocol is informative if every execution that is long enough is informative both for Alice and for Bob.

Thus while tokens do not have an explicit meaning in principle, in practice they may be viewed as statements about the game. If Bob has agreed to only pass if he holds card 3, and Bob passes, then Alice can infer that he holds that card.

Recall, however, that in the specification of the problem, all announcements must be “clear and truthful”. Rather than assigning truth values to tokens, we will capture this in our formalization of the second goal of the protocol: that Cath does not learn who possesses any card she does not hold.

Definition 2.3 (security). *An execution $((A, B, C), \vec{\alpha})$ of a protocol π is secure if for every $x \notin C$ there is*

1. *a deal $\delta' = (A', B', C)$ such that $x \in A'$ and $(\delta', \vec{\alpha})$ is also an execution of π , as well as*
2. *a deal $\delta'' = (A'', B'', C)$ such that $x \in B''$ and $(\delta'', \vec{\alpha})$ is also an execution of π .*

The protocol π is secure if every execution of π is secure.

Thus after a secure execution, Cath does not know who holds any given card that is not hers, even if she entirely knows the protocol and recalls every announcement that each of the players made. This avoids, for example, protocols based on “secret codes”, such as the above scenario where Bob passes when he has 3.

The goal of the current paper is to find informative, secure protocols for the generalized Russian cards problem, as specified above. All protocols we shall consider will follow a basic scheme, described in the next section.

3 The colouring protocol

In this section we shall describe the general colouring protocol, the central focus of this article. Before we do so, let us briefly describe some of the notation we shall use.

In this paper, p will denote a prime or a power of a prime, and \mathbb{F}_p the field with p elements. If d is any natural number, \mathbb{F}_p^d denotes the vector space of dimension d over \mathbb{F}_p . For a line $\ell = x + \lambda y$, we say y is a *directing vector* of ℓ . We denote by $\mathbb{F}_p^d[e]$ the set of all e -dimensional affine spaces in \mathbb{F}_p^d , that is, all sets of the form $x + V$, where V is an e -dimensional subspace of \mathbb{F}_p^d ; we call these *e -spaces*.

For natural numbers d, n we define $\sigma_d(n)$ to be the sum $n^{d-1} + n^{d-2} + \dots + n^0$. We know from basic algebra that

$$\sigma_d(n) = \frac{n^d - 1}{n - 1}.$$

This will be a very useful quantity to keep in mind; for example,

Lemma 3.1. *Given $x \in \mathbb{F}_p^d$, there are $\sigma_d(p)$ distinct lines passing through x .*

Let p be a prime or a prime power and $d \geq 2$. Assume that Alice holds as many cards as points in an e -space of \mathbb{F}_p^d (i.e. $a = p^e$) and that Alice, Bob and Cath together hold as many cards as points in the whole space (i.e. $a + b + c = p^d$). Let K be a set of k colours, identified with the numbers $1, \dots, k$. Colorings will be a crucial element in our protocol:

Definition 3.1 (Colouring). *A k -colouring of e -spaces is a function*

$$\xi : \mathbb{F}_p^d[e] \rightarrow K.$$

That is, ξ assigns a colour from $\{1, \dots, k\}$ to each subspace of \mathbb{F}_p^d of dimension e . Informally, the colouring protocol consists of the following four steps:

1. Alice maps all the cards into \mathbb{F}_p^d in such a way that her cards form an e -space.
2. Bob announces a *suitably chosen* k -colouring ξ of e -spaces.
3. Alice announces the colour of her hand according to ξ .
4. Bob announces Cath's cards.

Of course, we have yet to specify what a suitable colouring is. This will be the focus of the rest of this section. In order to guarantee that the protocol is informative (Alice and Bob can deduce the card deal after the protocol's execution), the colouring must be *distinguished*, as defined below. For it to be safe (Cath cannot learn any of Alice or Bob's cards), the colouring should also be *rich*. However, colourings which are merely rich and distinguished may give Cath too much information, and thus we will have to replace the condition of being distinguished by the stronger version of being *very distinguished*. Once we have defined these notions the next question is for which a, b, c and k such colourings exist, i.e., when the protocol is executable; this shall be the topic of later sections.

First let us focus on making the protocol be informative. Given a card deal (A, B, C) , we should design ξ in such a way that only A itself can be the e -space entirely contained in $A \cup C$ of whichever colour Alice announces. In this way, Bob can unequivocally identify A . But there may be many such spaces contained in $A \cup C$, and at the beginning of the protocol Bob has no way of telling them apart. Thus we arrive at the following:

Definition 3.2 (Distinguished colouring). *We say that a k -colouring ξ of e -spaces is distinguished for a set $E \subseteq \mathbb{F}_p^d$ if no two distinct e -spaces contained entirely in E have the same colour.*

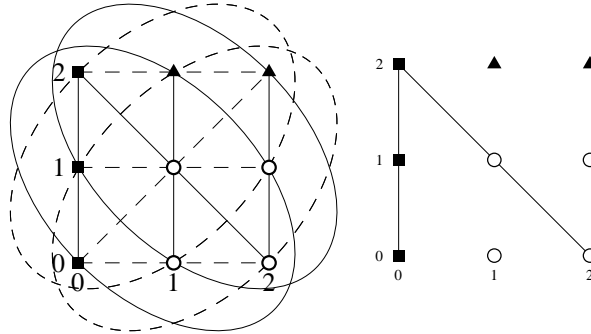


Figure 3: A simple 2-colouring.

Example 3.1. *Figure 3 illustrates the possible effects of a distinguished colouring. The left picture shows a 2-colouring that Bob announces after Alice maps the cards into \mathbb{F}_3^2 . Throughout the examples we will continue to use black squares for Alice's cards, white circles for Bob's and black triangles*

for Cath's, so that cards held by Alice or Cath are black-filled shapes. Alice's cards A form the line $\{00, 01, 02\}$. Cath's cards C are $\{12, 22\}$. The set $A \cup C$ also contains the line $\{02, 12, 22\}$. To enable Alice, by her later response, to distinguish both lines, Bob announces the 2-colouring in the left picture. It has two 'colours': solid lines and dashed lines. Ellipses in the figure are lines as well, e.g. $\{22, 10, 21\}$ is a dashed line.

Suppose Alice announces that her line is solid. Then, Bob will learn Alice's cards and he can announce Cath's cards. This may seem safe to announce, because now only one solid line is contained in $A \cup C$.

But the colouring that Bob announces is not safe. After Alice announces that her cards are a solid line, Cath discards all solid lines that meet some of her points. The right picture in Figure 3 shows the only two lines that Cath cannot discard. This makes Cath learn that Alice has 02 and that Bob has 10 and 21.

Hence, colourings that are merely distinguished will make the colouring protocol informative but not necessarily safe. To remedy this, we must have enough colours, and the colouring must be rich enough, so that for every card that Cath does not hold she should consider it possible both that Alice holds it and that Alice does not hold it.

Definition 3.3 (Rich colouring). *A k -colouring ξ is rich if for any c -set C , colour i , and point $x \notin C$, there is an i -coloured e -space A containing x that avoids C and there also is an i -coloured e -space A' not containing x that avoids C .*

Example 3.2. *Consider the trivial 1-colouring ξ on the left-side image in Figure 2 (all lines have the same colour). This colouring is distinguished for $A \cup C$, as this set only contains one line.*

It is also rich. To see this, note that given any c -set E and $x \notin E$, there are five lines passing through x , and thus one of them avoids E .

This covers one condition for richness; for the other, picking $y \neq x$ which is also not in E , we see that one line through y avoids $\{x\} \cup E$, and thus there is a line avoiding both x and E .

Rich and distinguished colourings are *almost* suitable, but we shall need an extra condition. Notice that Cath knows that Bob is to design the colouring so that it turns out to be informative. Thus, the colouring not only should be distinguished for the actual set of cards $A \cup C$ but also for every

set of cards that Bob wants Cath to consider as possible. These will be the sets with the same *hue* as $A \cup C$:

Definition 3.4 (Hue). *Let ξ be a k -colouring of e -spaces.*

Given $E, F \subseteq \mathbb{F}_p^d$, we write $E \approx_1^\xi F$ if there are e -spaces U, W of the same colour such that $U \subseteq E$, $W \cap (E \setminus U) = \emptyset$ and

$$F = (E \setminus U) \cup W.$$

We will say E, F are one tone apart.

We then let \approx^ξ be the reflexive and transitive closure of \approx_1^ξ , and define a hue to be an equivalence class under \approx^ξ .

Returning to Example 3.2, our trivial one-colouring is rich and distinguished, but it has one further property; for suppose that E has the same hue as $A \cup B$. Then, E can only contain one line (since it has only eight points) and thus ξ is *also* distinguished for E . Colorings with this property will be very useful and we shall say they are *very distinguished*.

Definition 3.5 (Very distinguished colouring). *We say that a k -colouring ξ is very distinguished for $E \subseteq \mathbb{F}_p^d$ if ξ is distinguished for every F of the same hue as E .*

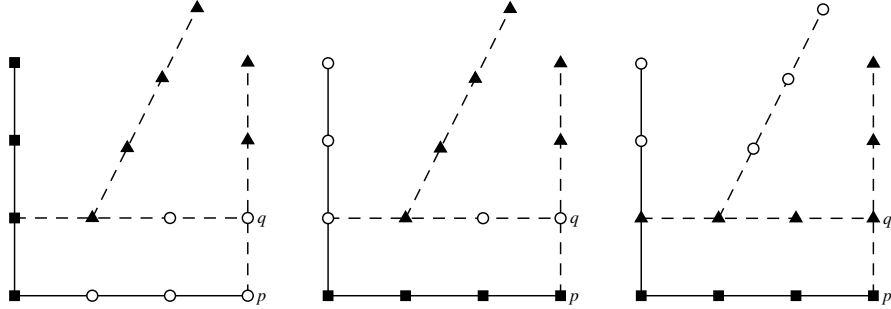


Figure 4: A 2-colouring which is distinguished but not very distinguished

Example 3.3. *Figure 4 shows an example of a 2-colouring in \mathbb{F}_4^n for some n . We have represented only some points and lines in the space. Let's suppose that the colouring is 6-rich. In the situation represented on the left, the colouring is distinguished. $A \cup C$ contains two lines with different colours. But the sets of points shown in the middle and right pictures are of the same*

hue as $A \cup C$, and the set of points in the right picture contains two lines of the same colour. Then our colouring is not distinguished in the right picture, so it is not very distinguished in the left one.

This means that the presented 2-colouring is not safe, even in the left picture. Cath may learn that the points p and q belong to Bob, reasoning as follows. Alice cannot have both points, because Alice's points are aligned, but she could have one of them, as can be seen in the center picture. However, if it were the case that Alice has one point (say, p), Bob should assign the line containing p, q a different colour to the other two lines in $A \cup C$, to keep Cath from learning that Bob has q . A similar reasoning applies to q , and thus Cath learns that Bob has both p and q .

With these considerations we know which kind of colouring Bob should use: a suitably chosen colouring is rich and very distinguished, and as we shall see, the protocol so defined is safe and informative.

Definition 3.6 (Colouring protocol).

1. Alice maps all the cards into \mathbb{F}_p^d in such a way that her cards form an e -space.
2. Bob announces a rich and very distinguished k -colouring ξ .
3. Alice announces the colour of her hand.
4. Bob announces Cath's cards.

Let us first see that the colouring protocol is indeed a protocol as defined in Section 2. To be precise, we must show that every announcement depends only on information available to the respective player. For example, suppose the protocol were to require that Bob instead of Alice maps all the cards into \mathbb{F}_p^d in such a way that Alice's cards form an e -space. Unless Bob is told what to say by an outsider, he cannot make that announcement knowingly: for any given mapping into \mathbb{F}_p^d , there are many subsets of size a of the complement of Bob's cards that are not an e -space under this mapping. Similarly, Bob cannot announce Cath's cards in the last step if he does not know them.

But this is not the case for the protocol we have described:

Lemma 3.2. *The colouring protocol is a protocol in the sense of Definition 2.1.*

Proof. We need to verify that at each stage each player has enough information to determine if their announcement is correct. Let us do this step by step:

1. *Alice maps all the cards into \mathbb{F}_p^d in such a way that her cards form an e -space.*

Alice knows her own cards, and this is sufficient for her to align them on an e -space; the other cards may then be distributed randomly.

2. *Bob announces a rich and very distinguished k -colouring ξ .*

That Bob can give such a colouring is not trivial, as it often will not exist. But suppose that a very distinguished colouring ξ exists². Then, Bob knows the cards in $A \cup B$ and thus can check that ξ is very distinguished by enumerating all $E \approx^\xi A \cup B$ and seeing whether ξ is distinguished for E ; richness can be tested in a similar way. Thus, by trial and error, Bob can find a suitable colouring ξ and announce ξ .³

3. *Alice announces the colour of her hand according to ξ .*

Alice knows what her cards are as well as Bob's colouring, so she can tell what color her hand is.

4. *Bob announces Cath's cards.*

Since ξ is distinguished for $A \cup C$, once Alice announces $i = \xi(A)$, Bob knows Alice's hand (it is the unique e -space in $A \cup C$ of colour i) and therefore Cath's cards are those that are left over.

□

It remains to check that the colouring protocol indeed provides a solution to the generalized Russian cards problem:

Theorem 3.1. *The colouring protocol is safe and informative, provided it is executable.*

²If ξ exists, we will say the protocol is *executable*. In later sections we shall analyze some cases where this always holds.

³The method we have described is extremely inefficient; it is better for Bob to construct ξ directly. In the following sections, we will discuss cases where he can do this.

Proof. The protocol is obviously informative given Bob's last announcement, so we focus on safety. It suffices to check that Cath cannot deduce Alice's cards even *after* Bob's announcement of ξ and Alice's announcement of $i = \xi(A)$.

First pick x that Cath does not hold. Because ξ is rich, there is an e -space A' with colour i passing through x and not meeting C . Further, note that $A \cup C \approx_1^\xi A' \cup C$, so that ξ is also very distinguished for $A' \cup C$. Then, it is possible from Cath's point of view that Alice holds all cards in A' and thus holds x .

The argument that Cath also considers it possible that Alice does not hold x is very similar. Since the set C has exactly c elements, there is a space A'' with colour i not meeting $C \cup \{x\}$, so that reasoning as above, it is conceivable from Cath's point of view that Alice's hand is A'' and Bob holds x . \square

It is pending to investigate for which a, b, c the colouring protocol is actually executable. In the remaining sections of this paper we shall explore this question in the "extreme" cases where Alice has a hyperplane (i.e. $e = d - 1$) and Alice has a line (i.e. $e = 1$), respectively.

4 Alice has a hyperplane

In this section we shall consider a relatively basic instance of the colouring protocol, the one closest to Atkinson's original proposal where we had $d = 2$. Here $d \geq 2$ is arbitrary, but $e = d - 1$, which means that Alice holds as many cards as points in a hyperplane of \mathbb{F}_p^d and thus $a = p^{d-1}$. Meanwhile, Cath holds few cards; less than p . This case is particularly simple because one can take $k = 1$ in the colouring protocol, i.e., it suffices to consider the trivial 1-colouring ξ assigning the same colour to every hyperplane of \mathbb{F}_p^d . As a consequence, steps 2 and 3 become superfluous, reducing it to two steps.

Definition 4.1 (Simplified colouring protocol).

1. Alice announces a map from the deck to \mathbb{F}_p^d , such that her cards correspond to a hyperplane.
2. Bob announces Cath's cards.

Example 3.2 is a case where the simplified colouring protocol works, but there are many more:

Theorem 4.1. *Assume that a, b, c, p, d satisfy the following conditions:*

1. p is a prime or prime power,
2. $a = p^{d-1}$,
3. $a + b + c = p^d$,
4. either $d = 2$ and $c \leq p - 2$ or $d \geq 3$ and $c \leq p - 1$.

Then, the simplified colouring protocol is executable.

Proof. In view of Theorem ??, we need only check that the trivial 1-colouring is suitable, i.e., that it is rich and very distinguished.

Distinctiveness. Let us first show that the 1-colouring ξ is very distinguished for $A \cup C$. Since ξ assigns the same colour to each hyperplane, this amounts to showing that there may only be one hyperplane in any E of the same hue as $(A \cup C)$. Fix such a set E . Note that cardinality is hue-invariant, so E contains $p^{d-1} + c$ points.

Meanwhile, suppose P, Q are two distinct hyperplanes. Then, $P \cup Q$ has at least

$$2p^{d-1} - p^{d-2}$$

points; this is because each hyperplane has p^{d-1} points and their intersection is a space of dimension at most $d - 2$. So it is sufficient to have

$$2p^{d-1} - p^{d-2} > p^{d-1} + c$$

or, equivalently,

$$c < p^{d-1} - p^{d-2} \tag{1}$$

to conclude that there is no way that E contains a second hyperplane.

It is then easy to show that (1) holds under our constraints.

Richness. We have to check that ξ is a rich 1-colouring. To this end, let E be a set with c elements and let x be a point not in E .

First of all, note that given $y \neq x$, there are $\sigma_{d-1}(p)$ hyperplanes touching both x and y . To see this, pick a hyperplane Q touching y but not x . Then, any hyperplane H touching both x and y intersects Q in a $d-2$ space H' , and conversely H' determines H . But H' is a hyperplane over Q through y , which means that there are $\sigma_{d-1}(p)$ values H' could take.

Since E has c points there are at most $c\sigma_{d-1}(p)$ hyperplanes touching E and meeting x , whereas there are $\sigma_d(p)$ hyperplanes touching x in total. So, it is sufficient to have that

$$\sigma_d(p) = p\sigma_{d-1}(p) + 1 > c\sigma_{d-1}(p)$$

or, equivalently,

$$c < p + \frac{1}{\sigma_{d-1}(p)}$$

to conclude that at least one hyperplane through x does not meet E , fulfilling the first condition of Definition 3.3. However, this readily follows from our constraints, since $c < p$.

As for the second condition, on the one hand, there are $p\sigma_d(p)$ distinct hyperplanes in total in \mathbb{F}_p^d : there are $\sigma_d(p)$ normal vectors for a hyperplane and each hyperplane has p parallel hyperplanes. On the other hand, there are strictly less than $(c+1)\sigma_d(p)$ hyperplanes meeting $E \cup \{x\}$, since if $z \in E \cup \{x\}$ then there are $\sigma_d(p)$ hyperplanes passing through z and at least one hyperplane is counted twice. So, it is sufficient to have

$$p\sigma_d(p) \geq (c+1)\sigma_d(p)$$

or, equivalently, $c \leq p-1$ to conclude that at least one hyperplane does not meet $E \cup \{x\}$. But this is already a constraint. \square

It is not hard to find parameters satisfying the conditions of Theorem 4.1. At the low end are the triples $(a, b, c) = (3, 5, 1)$, $(4, 10, 2)$, $(4, 11, 1)$, $(5, 17, 3)$, $(5, 18, 2)$, and $(5, 19, 1)$; the case $(5, 17, 3)$ was used for illustration in the introductory section and Example 3.2.

If we look at larger numbers, we see that Cath needs to have a great deal fewer cards than Alice, and that Bob tends to have quite a few more. Given that Alice has $a = p^{d-1}$, Cath has in the order of p , and Bob has less than p^d , we have $b = O(ac)$. This improves on previous results, since the generalized

Atkinson protocol from [1] uses $b = O(a^2)$, independently of the value of c (which might be much smaller than a). We remark that all cases for $c = 1$ are already covered in prior work [1, 2].

We have made a few simplifying assumptions in this section, for the sake of exposition, but there are some straightforward generalizations that could be made. First, we could drop the assumption that Alice holds *exactly* a prime power of cards; if she has less, the protocol may be tweaked so that she holds only a portion of the hyperplane. In this case, Cath must still hold less cards than Alice; this is done in [1] for the case $d = 2$.

Further, we have only dealt with the case where Alice arranges her cards in a hyperplane. This maximizes the number of cards that Alice can hold; however, essentially by the same arguments it could be checked that the simplified colouring protocol also works when Alice has any e -dimensional subspace of \mathbb{F}_p^d with $1 \leq e < d$. Nevertheless, the bounds for the inequalities become more complicated and, in any case, given that we use a 1-colouring, we can only derive the existence of protocols for triples (a, b, c) with $c < a$. For k -colourings for $k > 1$, the picture looks a great deal brighter and more challenging.

5 Alice has a line

In this section we shall consider another extreme case: when Alice's cards only form a line. Despite the apparent symmetry, this case is much more involved than the previous and will require the full machinery of the colouring protocol.

As before, let p be a prime or a prime power and $d \geq 2$. We will assume that $e = 1$, that is, Alice has as many cards as points in a line of \mathbb{F}_p^d . This is an important case because it represents when Alice has minimal information and, as we shall see, it will allow us to derive the existence of protocols for triples (a, b, c) with $c \gg a$. For this, the constriction of a non-trivial k -colouring will be crucial.

In what follows we will look for conditions to guarantee the existence of a rich and very distinguished k -colouring for some number of colours k . First, let us introduce the notion of *density*:

Definition 5.1. *Say a k -colouring of lines ξ has density m if, given a point $x \in \mathbb{F}_p^d$ and a colour i , there are at least m i -coloured lines through x .*

There is a close connection between density and richness; to be precise, a colouring that is dense enough is automatically rich.

Lemma 5.1. *If ξ is a k -colouring of density $c + 2$, then ξ is rich.*

Proof. Let E be a subset of \mathbb{F}_p^d with c elements. Fix a colour i and a point $x \notin E$. We note that if ℓ, h are two distinct lines passing through x , then $\ell \cap h = \{x\}$. Therefore, E contains the disjoint union

$$\bigcup \{E \cap \ell : x \in \ell \text{ and } \xi(\ell) = i\}.$$

It follows that for some ℓ with $\xi(\ell) = i$ and $x \in \ell$, $E \cap \ell$ must be empty, otherwise E would have at least $c + 2$ elements.

Similarly, if we pick $y \notin E$ different from x , we see that there is an i -coloured line through y not meeting $E \cup \{x\}$, satisfying the second requirement. \square

Thus in order to construct rich colourings, we may focus on constructing dense colourings; this is not too difficult, as witnessed by the following:

Lemma 5.2. *Let ℓ_1, \dots, ℓ_k be distinct lines of $\mathcal{V} = \mathbb{F}_p^d$ and assume that $\sigma_d(p) \geq k(m + 1)$. Then, there is a k -colouring ξ of density m such that for $i \leq k$, $\xi(\ell_i) = i$.*

Proof. There are $\sigma_d(p) \geq k(m + 1)$ non-collinear vectors in \mathcal{V} , and hence we can pick a set D of mk non-collinear vectors which are not directing vectors of any of the lines ℓ_i . Partition D into k disjoint sets D_i of m elements. Then, given a line $h \in \mathcal{V}$, put $\xi(h) = i$ if either $h = \ell_i$ or h has directing vector in D_i for some $i \leq k$. Otherwise put, for instance, $\xi(h) = 1$. It is easy to see that ξ satisfies the desired properties. \square

This will be sufficient for finding rich colourings. Now our goal is to construct a very distinguished k -colouring for $A \cup C$. As with richness, we will do so by introducing a stronger, approximate notion – that of a *perfect colouring*. It is not easy to tell under which conditions very distinguished colourings exist or how one may go about finding one, but finding perfect colourings will be straightforward.

Perfect colourings do have the disadvantage that they are not hue-invariant. To deal with this issue, we will first need an intermediate concept: that of *critical colourings*. Every perfect colouring is critical and every critical colouring is very distinguished. Perfect colourings are the easiest to identify,

but critical colourings are easier to work with than either perfect or very distinguished colourings.

Let us then begin by defining critical colourings:

Definition 5.2 (critical colouring). *Given $E \subseteq \mathbb{F}_p^d$, we say that a k -colouring ξ is critical for E if there exists a set $L = \{\ell_1^*, \dots, \ell_n^*\}$ of lines of different colours such that, for every line $h \subseteq \mathbb{F}_p^d$, we have*

$$\#((h \cap E) \setminus \bigcup_{i \leq n} \ell_i^*) < p - k,$$

where $\#S$ stands for the cardinality of a set S . We will say the lines in L are ξ -critical lines for E .

The notion of critical colouring in Definition 5.2 captures an important difference between the 2-colourings in Figures 4 and 5. The 2-colouring in Figure 4 is not critical for $E = A \cup C$, as for any set of lines L that we can select, there is a line h such that

$$\#((h \cap E) \setminus \bigcup L) \geq 2 = p - k,$$

as the reader may verify by examination.

On the other hand, the colouring in the left-hand side of Figure 5 is critical for $E = A \cup C$, the union of the two lines and the fragment. We select L as the two complete lines in E . Then, for any line h , the property of Definition 5.2 holds. In particular, the line h with the three holes is the line outside of L with most points in E . For that line,

$$\#((h \cap E) \setminus \bigcup L) = p - 3 < p - 2.$$

Recall Example 3.3, where we showed that the colouring in Figure 4 is insecure. Intuitively, the insecurity of a k -colouring (in Figure 4 we have $k = 2$) is produced because $A \cup C$ contains k lines, along with a line fragment ℓ with k or less gaps – observe the line missing p and q in Figure 4. Then, though the k -colouring is distinguished, it might not be very distinguished, as we may be able to travel several tones to move the k lines and fill all the gaps in ℓ , thus generating $k + 1$ lines and repeating a colour.

However, when $A \cup C$ contains k or less lines and all fragments have more than k points missing, then a distinguished k -colouring ξ is always very distinguished. Figure 5 shows an example of this situation.

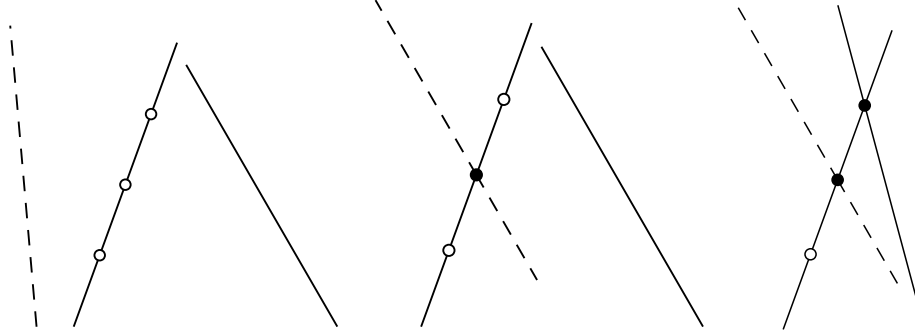


Figure 5: A critical 2-colouring

Example 5.1. *In the left-hand side of Figure 5, $A \cup C$ contains two lines and a fragment with three or more points missing. Alice has one of these lines, and Cath has the other line plus the segment. Then, a tone corresponds to moving a line to an empty position of the same colour, and it is not possible to arrange the two lines in $A \cup C$ in such a way that they fill the three gaps in the fragment. Thus there is no configuration of the same hue for which ξ is not distinguished, so that ξ is very distinguished.*

The above considerations suggest that critical colourings are very distinguished, and indeed this will turn out to be the case. Before we show this, let us make a simple observation:

Lemma 5.3. *If ξ is a critical k -colouring for E and $\ell \subseteq E$, then ℓ is a ξ -critical line for E , independently of how the other critical lines are chosen.*

Proof. Let $\ell_1^*, \dots, \ell_n^*$ be ξ -critical lines for E . Notice that since they are lines of different colours, we have $n \leq k$. If ℓ is not ξ -critical then for every $i \leq n$, $\ell \cap \ell_i^*$ is either empty or a singleton. It therefore follows that

$$\#((\ell \cap E) \setminus \bigcup L) = \#(\ell \setminus \bigcup_{i \leq n} \ell_i^*) \geq p - n \geq p - k,$$

which contradicts the definition of a critical k -colouring. \square

Now we will check that critical colourings are very distinguished. For this, it suffices to show that they are distinguished and hue-invariant; the former is straightforward, the latter rather involved.

Lemma 5.4. *Every critical k -colouring for E is distinguished for E .*

Proof. From Lemma 5.3 it follows that if $\ell \subseteq E$ then it is critical; but there is at most one critical line of each colour so there cannot be $h \neq \ell$ of the same colour both contained in E . \square

Lemma 5.5. *Suppose ξ is a critical k -colouring for E with $k < p$ and F has the same hue as E . Then, ξ is also a critical colouring for F .*

Proof. We shall prove this by induction on the number of tones between E and F . The base case ($F = E$) is vacuous. For the inductive step, suppose $F = (G \setminus \lambda_1) \cup \lambda_2$ with $\xi(\lambda_1) = \xi(\lambda_2) = j$, where by induction there are ξ -critical lines $\ell_1^*, \dots, \ell_n^*$ for G with $n \leq k$. Observe that $\ell_j^* = \lambda_1$; indeed, $\lambda_1 \subseteq G$, so that by Lemma 5.3, $\lambda_1 = \ell_i^*$ for some i . But $\xi(\lambda_1) = j$, and therefore $i = j$.

Our goal is to show that ξ is also critical for F ; we will do this by proving that the lines h_1^*, \dots, h_n^* defined by $h_i^* = \ell_i^*$ for $i \neq j$ and $h_j^* = \lambda_2$ are critical. For this it will suffice to check that if ℓ is any line,

$$(\ell \cap F) \setminus \bigcup_{i \leq n} h_i^* \subseteq (\ell \cap G) \setminus \bigcup_{i \leq n} \ell_i^*; \quad (2)$$

this inclusion would then imply that

$$\#((\ell \cap F) \setminus \bigcup_{i \leq n} h_i^*) \leq \#((\ell \cap G) \setminus \bigcup_{i \leq n} \ell_i^*) < p - k,$$

showing that h_1^*, \dots, h_n^* (and hence ξ) are critical for F .

To establish (2), pick $x \in (\ell \cap F) \setminus \bigcup_{i \leq n} h_i^*$. It is obvious that $x \in \ell \cap G$, except in the case that $x \in \lambda_2$. But $\lambda_2 = \bar{h}_j^*$, so this cannot be, and therefore we always have $x \in \ell \cap G$.

Next, we need to check that $x \notin \ell_i^*$ for any $i \leq k$. This is obvious if $i \neq j$, since $\ell_i^* = h_i^*$. Thus it remains to rule out that $x \in \ell_j^*$. If we had $x \in \ell_j^* = \lambda_1$, we would also have that $x \in \lambda_1 \setminus h_j^* = \lambda_1 \setminus \lambda_2$. But F does not intersect this set, so this is impossible.

We conclude that (2) holds, and thus ξ is critical for F , as desired. \square

As promised, we now have the following:

Lemma 5.6. *Every critical colouring is very distinguished.*

Proof. If ξ is critical for E , then by Lemma 5.5, it is also critical for every set of the same hue as E ; thus, by Lemma 5.4, it is also distinguished for every such set. \square

We have seen that in order to construct very distinguished colourings, it suffices to construct critical colourings. This has the advantage that the notion of being critical depends only on a set E and not on the entire hue of E . However, it is still not entirely obvious when exactly critical colourings exist or how one is to go about building one.

This is where perfect colourings come into play. Although less well-behaved than critical colourings, they are very easy to identify, and every perfect colouring is automatically critical.

Definition 5.3 (perfect k -colouring). *Given $E \subseteq \mathbb{F}_p^d$, let $L_m(E)$ denote the set of all lines ℓ such that $\#(\ell \cap E) \geq m$.*

We say that a k -colouring ξ is perfect for E if different elements of $L_{p-k}(E)$ have different colours.

Perfect colourings are thus quite easy to identify and construct, yet they are always very distinguished:

Proposition 5.1. *If ξ is a perfect colouring for E , then ξ is very distinguished for E .*

Proof. First we note that ξ is critical, since we can take all of $L_{p-k}(E)$ as critical lines, given that they are all of different colour. Then, by Lemma 5.6, we have that ξ is very distinguished, as required. \square

Now for the main result of this section:

Theorem 5.1. *Assume that a, b, c, d, k satisfy the following conditions:*

1. *a is a prime or a prime power,*
2. *$a + b + c = a^d$,*
3. *$k < a$,*
4. *for every $S \subseteq \mathbb{F}_a^d$ with $\#S \leq a + c$, we have $\#L_{a-k}(S) \leq k$;*
5. *$\sigma_d(a) \geq k(c + 3)$.*

Then, the colouring protocol is executable.

Proof. By assumption, $\#L_{a-k}(A \cup C) \leq k$, so Bob can enumerate $L_{a-k}(A \cup C)$ by $\vec{\ell} = \langle \ell_1, \dots, \ell_n \rangle$, with $n \leq k$. Then, by Lemma 5.2, there exists a colouring ξ with density $c + 2$ and such that $\xi(\ell_i) = i$, which by construction is perfect for $A \cup C$, so that by Proposition 5.1, it is also very distinguished. Further, by Lemma 5.1, we see that ξ is rich, as needed. \square

The above proof should be seen as a theoretical argument that very distinguished colourings exist under the above conditions – but never as an algorithm for constructing them. The reason is as follows. Perfect colourings are not hue-invariant. Thus if Bob were *always* to choose a perfect colouring, Cath may be able to infer additional information from this. Colourings should be chosen homogeneously within a hue, either by picking them randomly each time or by selecting a uniform representative a priori. Whether there are good algorithms for doing this is a question we shall leave open.

5.1 Some bounds

The conditions given by Theorem 5.1, while rather general, remain somewhat implicit. In this subsection we shall compute some explicit bounds on the parameters which guarantee that these conditions are met. The computations we will make are a bit rough, but will nevertheless give us a large family of parameters for which the protocol is guaranteed to work.

They are based on the following counting lemma:

Lemma 5.7. *If a set $E \subseteq \mathbb{F}_p^d$ is such that $\#E < (k + 1)(p - k) - (k+1)k/2$, then*

$$\#L_{p-k}(E) \leq k.$$

Proof. We argue by contrapositive, assuming that $\#L_{p-k}(E) > k$.

Let $\ell_1, \dots, \ell_{k+1}$ be distinct lines such that $\#(E \cap \ell_i) \geq p - k$. Then, we have

$$\begin{aligned} \#E &\geq \# \bigcup_{i \leq k+1} (\ell_i \cap E) \\ &\geq \sum_{i \leq k+1} \#(\ell_i \cap E) - \sum_{i < j \leq k+1} \#(\ell_i \cap \ell_j) \\ &\geq (k + 1)(p - k) - (k+1)k/2. \end{aligned}$$

\square

Thus in view of Theorem 5.1, in order to find suitable parameters, it suffices to solve the system of inequalities

1. $a + c < (k + 1)(a - k) - (k+1)k/2$
2. $\frac{a^d - 1}{a - 1} \geq k(c + 3)$

or, simplifying a bit,

1. $c < ak - 3(k+1)k/2$
2. $a^d > k(a - 1)(c + 3).$

From this we immediately obtain the following ‘asymptotic’ result:

Theorem 5.2. *For a large enough, the above inequalities hold for*

1. $c < O(a^{3/2})$ and $d = 3$,
2. $c < O(a^2)$ and $d = 4$.

Proof. For the first result, set $k \approx \sqrt{a}$ and $c < a^{3/2}/2$.

Then, we have that

$$ak - \frac{3k(k+1)}{2} = a^{3/2} + O(a),$$

which for large a is greater than $a^{3/2}/2$.

Meanwhile,

$$k(a - 1)(c + 3) = a^{3/2} + O(a^2),$$

which for large a is bounded by a^3 .

The second is similar; here, set $k \approx a/2$ and $c \approx a^2/9$. □

A nice conclusion we obtain from the above result is that indeed c can be larger than a by any order of magnitude we desire, provided a is large enough:

Corollary 5.1. *Given any natural number N , there exist a, c such that $c/a > N$ and the colouring protocol is executable, sound and informative for $(a, a^3 - a - c, c)$.*

Proof. If $a \gg N^2$ then $a^{3/2} = (a^{1/2})a \gg Na$ and, by Theorem 5.2.1, the required inequalities hold and the protocol is executable. \square

Note that we may use Theorem 5.2.1 or Theorem 5.2.2 depending on whether we wish to keep b relatively small with respect to a or a relatively small with respect to c . In either case, $b = O(c^2)$. Note also that our computations are heuristic and do not rule out the possibility of better bounds being obtained.

6 Conclusions and further research

The colouring protocol we have presented gives a new and flexible solution to the generalized Russian cards problem. Although inspired on Atkinson’s protocol, the introduction of colourings allows us to apply it in many more instances. In particular, our protocol solves the problem in many cases where the eavesdropper has more cards than one of the players, and is the first known solution to achieve this. In fact, if the generalized Russian cards problem is to be understood as *Find triples (a, b, c) for which a sound and informative protocol exists*, then the current work is a giant stride over what had been previously achieved.

The computations in the case that Alice has a hyperplane could be carried out in much the same way over projective rather than vector spaces, thus obtaining a solution that is closer to Atkinson’s. Our choice of working on vector spaces was due to the fact that, in the case that Alice has a line, many of the constructions seemed to work out more easily. However, it might be possible, and would be interesting, to study the projective version of the colouring protocol.

Actually, there are many variations that could be analyzed and might yield important results. We only considered the “extreme” cases where Alice has either a line or a hyperplane, and while one might argue that these are important (Alice’s information is either minimal or maximal), a more thorough analysis which includes intermediate cases should be pursued, along with other variations: Alice may have more than one e -space, there may be more players, Cath may be allowed to learn a few of the cards, etc. Along these lines, a particularly promising direction would be to replace linear spaces by other algebraic curves. This could, potentially, reduce the size of the whole space (and hence Bob’s hand) without compromising the existence of suitable colourings.

A different direction to pursue involves cases where either a or $a+b+c$ are not prime powers. There are already standard techniques to deal with these; one finds a prime which is not much larger than the desired parameter and works with that instead. Such techniques have already been used to extend a different protocol to many new triples in [2] but have not been worked out in our context.

Meanwhile, the generalized Russian cards problem may have a recreational flavour to it, but this is misleading; secret-exchange protocols beg for serious applications in secure communication. Unfortunately, concrete applications have not yet been developed, even theoretically. One could argue that part of the reason for this is that no sufficiently general solution to the problem was available; one could then go on to argue that the present work changes this situation.

Protocols based on the generalized Russian cards problem have an advantage over most traditional encryption methods in that they are “unconditionally secure”, meaning that an eavesdropper is unable to decypher messages even when granted unlimited computational capacity. The drawback is that it presupposes a secure “dealing stage”, which in most potential applications would not be available.

Real-world implementation of these protocols would also require an additional computational and probabilistic analysis. What is the complexity of running the colouring protocol? Are there good algorithms for finding suitable colourings? Even if Cath does not learn any cards, what is the probability that she guesses them correctly?

To summarize, there is much to be done indeed!

Acknowledgements

This research was supported by the project *Logics for Unconditionally Safe Protocols*, Excellence Research Project of the Junta de Andalucía P08-HUM-04159.

References

- [1] M.H. Albert, R.E.L. Aldred, M.D. Atkinson, H. van Ditmarsch, and C.C. Handley. Safe communication for card players by combinatorial

- designs for two-step protocols. *Australasian Journal of Combinatorics*, 33:33–46, 2005.
- [2] A. Cordon, H. van Ditmarsch, D. Fernández, J.J. Joosten, and F. Soler. A secure additive protocol for card players. To appear in *Australasian Journal of Combinatorics*. <http://arxiv.org/abs/1111.0156>, 2012.
 - [3] M.J. Fischer and R.N. Wright. Bounds on secret key exchange using a random deal of cards. *Journal of Cryptology*, 9(2):71–99, 1996.
 - [4] T. Kirkman. On a problem in combinations. *Camb. and Dublin Math. J.*, 2:191–204, 1847.
 - [5] K.S. Makarychev and Yu.S. Makarychev. The importance of being formal. *Mathematical Intelligencer*, 23(1):41–42, 2001.
 - [6] T. Mizuki, H. Shizuya, and T. Nishizeki. A complete characterization of a family of key exchange protocols. *International Journal of Information Security*, 1:131–142, 2002.
 - [7] A. Stiglic. Computations with a deck of cards. *Theoretical Computer Science*, 259(1–2):671–678, 2001.
 - [8] D.R. Stinson. *Combinatorial Designs – Constructions and Analysis*. Springer, 2004.
 - [9] H. van Ditmarsch. The Russian cards problem. *Studia Logica*, 75:31–62, 2003.
 - [10] H. van Ditmarsch and F. Soler-Toscano. Three steps. In J. Leite, P. Torroni, T. Ågotnes, G. Boella, and L. van der Torre, editors, *Computational Logic in Multi-Agent Systems - 12th International Workshop, CLIMA XII. Proceedings*, pages 41–57. Springer, 2011. LNCS 6814.